Comparison on BIOS between UEFI and Legacy

Abstract

The BIOS (Basic Input/Output System) connects the hardware with the system software. The system BIOS is between the system hardware and the system software, defining a firmware interface to ensure the computer available for use after power-on into OS environment.

The legacy BIOS was developed two decades ago, and although it had improved a lot since then, basically it was based on the structure of 16-bit processor mode, 1 MB addressable space, PC AT[1] hardware dependencies, etc. Nowadays PC hardware platforms have had amazing changes and OS has also evolved from the early MS DOS1.0 to today Windows 7, Windows 8, and so on. But, as a Key component, BIOS in the whole system still keeps its original scheme without many changes for the past twenty years, which has become a serious obstacle for PC advancement. Thus, a new firmware structure was presented to meet the current powerful OS and hardware complexity, providing us a PC device with high performance and low power consumption.

In order to upgrade PC advancement, an initial effort to solve these concerns was made by Intel, defining a new BIOS firmware interface, called EFI (Extensible Firmware Interface) in Spring 2000 IDF (Intel Developer's Forum). EFI is viewed as a significantly improved replacement of the old legacy BIOS firmware interface making PC faster and more efficient. The EFI specification is now managed by the Unified EFI Forum and is officially known as UEFI (Unified EFI).

BIOS Evolution History

Why we need to have a new BIOS structure?

Due to the dissatisfaction of old PC performance, we need a powerful BIOS to provide us a better environment to support PC hardware and software, and further to make PC stronger. EFI BIOS is proposed as the solution at the time. After continually changing in BIOS structure over years, UEFI BIOS has become a new trend of BIOS in the PC industry.

Now let's take a look at the difference between the designs of these two kinds of BIOS.

[1] Trademark acknowledge:
PC-AT is a registered trademark of International Business Machines Corp.
Windows is a registered trademark of Microsoft Corp.
Intel is a registered trademark of Intel Corp.
All product and company names are trademarks or registered trademarks of their respective holders.

© 2012 MilDef Crete Inc. All rights reserved.

Check with their Boot-Up Process

First, we check their boot-up process from power-on to operating system loading.

On the Legacy BIOS:

When you press the power button on a computer, the BIOS in this machine starts to perform the following procedures before getting into OS environment.

1. **Initialization:**
   Simply initialize CPU, Chipsets, standard parts of the computer system for basic preload work. All these actions are intended to use FDD (controlled by Super I/O) or CD Drive (controlled by IDE/USB) to rescue BIOS boot block in case of BIOS boot failure.

2. **POST（Power On Self Test）:**
   Execute a diagnostic/reliability test of the system hardware components, VGA, RAM and other option ROM programs, etc. in order to make sure a good quality of components before working for you.

3. **Keep a record of the system Configuration:**
   According to its own system resource table, BIOS will check the whole system to see what devices are installed to the computer. It might show on the screen which device is detected and register it on resource table for future reference.

4. **Provide Interrupt Service Routines:**
   Hardware is active by interrupt, and Software utilizes the interrupt vector to find its respective hardware to work for it, so BIOS prepares an interrupt vector table for OS or Apps to call in the future.

5. **Boot the operating system:**
   After finishing the system check-up and resource allocations, BIOS begins to search for a boot device in a pre-set boot sequence to load OS for use.

On the UEFI BIOS:

UEFI BIOS development is based on the specification interface of UEFI defined by Unified EFI Forum. Its Power-on process stages are presented as below:

1. **SEC Phase (Security)：**
   SEC is the first stage after Power-On, and its main task is to move SP (Stack Pointer) of CPU to CPU internal cache, i.e. Cache as RAM. Later it can proceed on different verifications for security according to the requirement for the system.

© 2012 MilDef Crete Inc. All rights reserved.

2. **PEI Phase (Pre-EFI Initialization)：**
   This stage is similar to the Legacy BIOS on initialization, beginning to initialize CPU, Chipset and Memory in preparation for setting up an environment for the next stage to load device drivers.

3. **DXE Phase (Driver Execution Environment)：**
   Most parts of system initialization are performed at this phase. DXE's main purpose is to set up a communication platform between EFI drivers and their hardware so that they can go on the necessary initialization by their configurations such as dual core, quad core, PCI, USB, SATA, etc., starting to be initialized at this time.

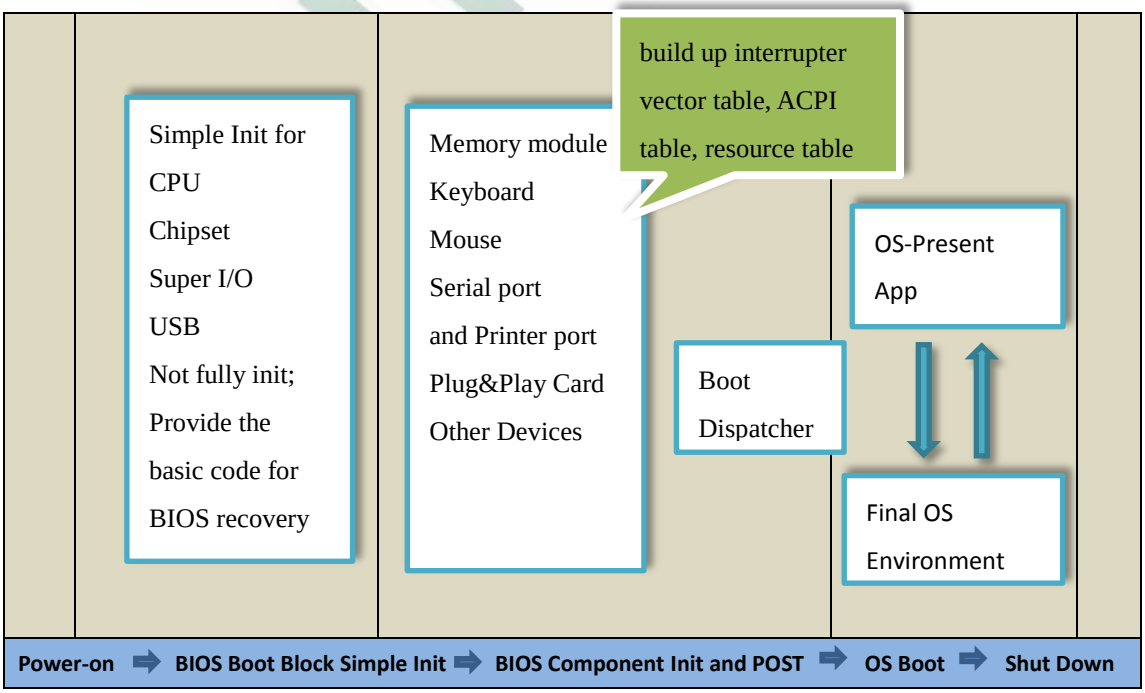
4. **BDS Phase (Boot Device Select):**
   In the BDS phase, users can enter Set-Up Menu to choose a device as a boot device when it is detected on the boot sequence.

5. **TSL Phase (Transient System Load):**
   After Operating System is loaded, OS then takes over to control the whole system. In addition, you can also choose to enter UEFI Shell in BSD phase in order to get into a simple command line for debugging or maintenance.

Overview on Diagram Flow-Chart for Both BIOS

Here shows on boot-up process in graphs for your better understanding of their flow.

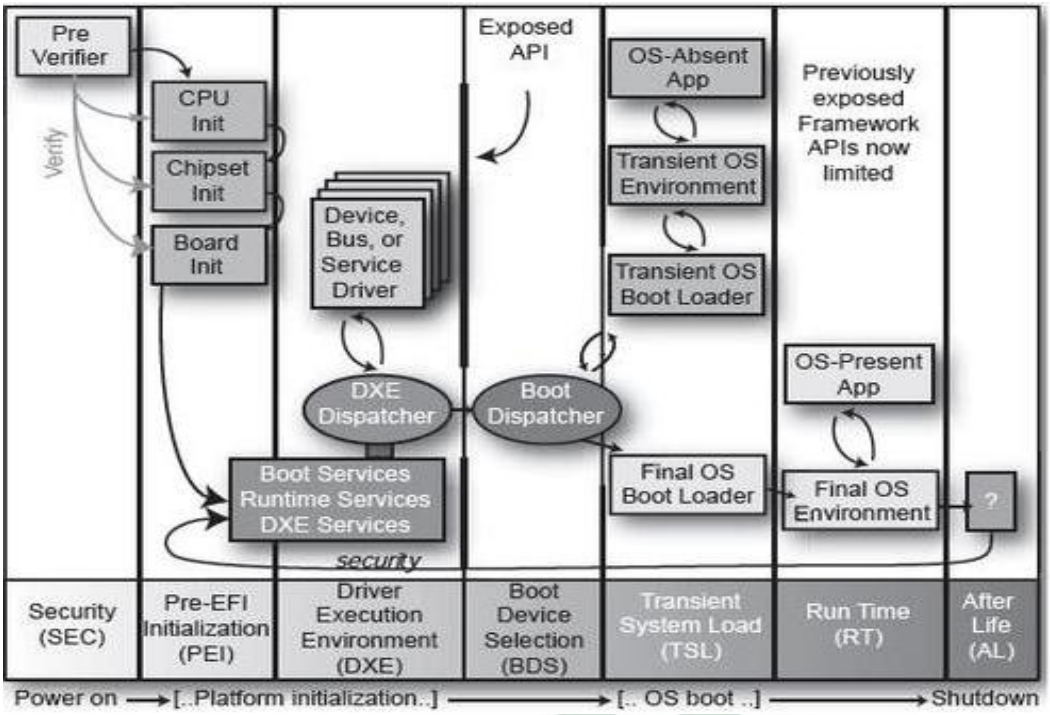
Diagram for Legacy BIOS Operational Model on below[2]:



[2] Adapted from the site: http://jay-fva.blogspot.tw/2010/12/uefi-%E4%BB%8B%E7%B4%B9.html

© 2012 MilDef Crete Inc. All rights reserved.

Diagram for EFI BIOS Operational Model on below[3]:



The Comparison on ingredients between Legacy and UEFI BIOS[4]:

	Legacy BIOS	EFI
Language	Assembly	C (99%)
Resource	Interrupt Hardcode Memory Access Hardcode I/O Access	Driver \ Protocols
Processor	x86 16-bits	CPU Protected Mode (Flat Mode)
Target	Binary Code	Removable Binary Drivers
Expand	Hook Interrupt	Load Driver
OS Bridge	ACPI (SMI, INT Service)	Run Time Driver Service AED (ACPI EFI Protocol Driver) (ACPI, SMI)
3rd Party ISV & IHV	Bad for Support	Easy for Support and for Multi Platforms

Note: ISV = Independent Software Vendor. IHV = Independent Hardware Vendor.

The Benefit of UEFI BIOS

1. **Enhance BIOS efficiency**

   The Legacy BIOS still keeps the way of 16 bit execution mode while CPU has entered 32/64 bit era. In this way, new CPUs must retain this 16 bit mode internally to

[3] The diagram is quoted from AMI (American Megatrends Incorporated) training course.
[4] The table is quoted from AMI (American Megatrends Incorporated) training course.

© 2012 MilDef Crete Inc. All rights reserved.

downgrade its efficiency for its backward compatibility on the old BIOS. However, after UEFI BIOS was presented, it tried to enter Protected Mode (Flat Mode) from Real Mode as soon as possible and to allow BIOS to access all resources on the system immediately after a machine power-on. Such processes make it possible that a computer boot-up becomes faster than ever.

2. **Easy for Development and Maintenance.**
   99% of UEFI BIOS codes are built in high-level C language, so it is better to maintain or create new functions for developers than those using assembly code in the old BIOS.

3. **Provide Flexible Interface Environment to reduce compatibility occurrence for later software upgrade.**
   EFI driver has a flexible driver module architecture, which can expand driver and interface continuously without needs to rewrite the whole code, so it is not necessary to consider compatibility issue after system upgrade.

4. **Avoid using absolute address**
   UEFI BIOS uses the way to load EFI driver during DXE phase to initialize hardware devices, other than hardware code access so that makes device installation more portable and flexible on the different systems. This also avoids unnecessary address conflict to cause a compatible problem.

Backward Compatible Issue of UEFI BIOS to the Legacy OS

A general UEFI BIOS mostly includes a CSM module (Compatibility Support Module) to support the Legacy OS and Legacy Option ROMs. If you try to install old hardware modules in the system, you'd better choose an OS with the legacy support to get less compatibility issues.

Conclusion

UEFI is an industry specification, which is referred to as having more flexible, extensible and portable characteristics to communicate between hardware and software. If we have a system with an UEFI BIOS, UEFI OS Installation and UEFI drivers, you will find less compatible problems and easier for later system upgrade. For PC, however, in the industry and military world, old option cards applied are still very popular. If someone hopes to use new UEFI BIOS to obtain benefits as mentioned above, they will finally find that the big problems of compatibility could be worse than ever in the legacy BIOS.

Author

Smile Chang, Software Manager, R & D Department, MilDef Crete Inc.

© 2012 MilDef Crete Inc. All rights reserved.